PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07D 7/00 — A1

(11) International Publication Number: WO 97/24699

(43) International Publication Date: 10 July 1997 (10.07.97)

(21) International Application Number: PCT/GB95/03051

(22) International Filing Date: 29 December 1995 (29.12.95)

(71) Applicant *(for all designated States except US)*: S. E. AXIS LIMITED [GB/GB]; Centre Court, 1301 Stratford Road, Hall Green, Birmingham B28 9AP (GB).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: KARIAKIN, Youry D. [BY/BY]; 13-89 Znianskaya Street, Minsk, 220100 (BY).

(74) Agent: LANGNER PARRY; 52/54 High Holborn, London WC1V 6RR (GB).

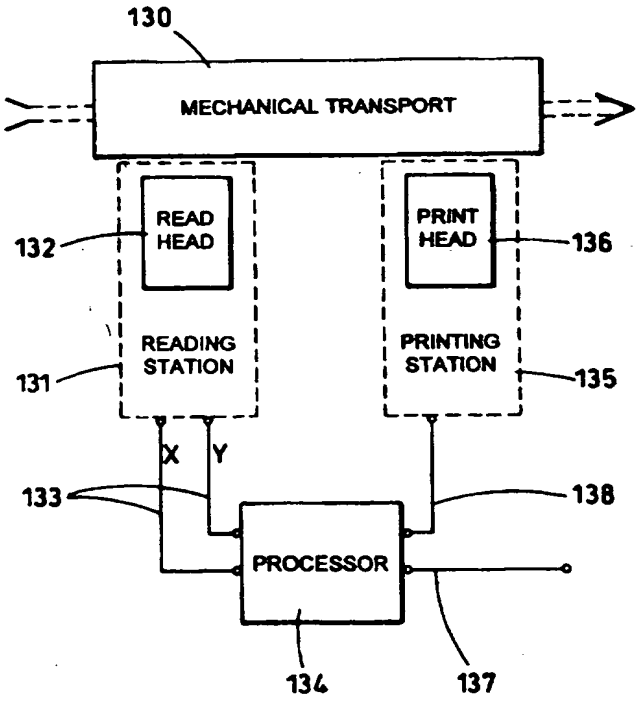
(81) Designated States: AU, BB, BG, BR, CA, CN, CZ, EE, FI, HU, IS, JP, KR, KZ, LK, LT, LV, MD, MX, NO, NZ, PL, RO, TT, UA, UG, US, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: AUTHENTICATION OF ARTICLES

(57) Abstract

A method and apparatus for authenticating articles using the steps of determining a distinguishing physical or chemical characteristic of an article, encoding that physical or chemical characteristic as an encoded characteristic, encrypting the encoded characteristic so derived to form an encrypted representation using a secret encryption key, applying that encrypted representation to the article, subsequently authenticating the article by redetermining the physical or chemical characteristic and reading and decrypting the encrypted representation and comparing the resulting encoded characteristic of the recorded physical or chemical characteristic with the redetermined physical or chemical characteristic to determine the authenticity of the article.



RNSDOCID: WO 9724699A1>

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia
AT	Austria
AU	Australia
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CS	Czechoslovakia
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgystan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakhstan
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam

AUTHENTICATION OF ARTICLES

Field of the Invention

This invention relates to cost-effective authentication of articles and hence assists to protect a wide range of articles from forgery and counterfeiting.

Background of the Invention

Protection against forgery and counterfeiting is a requirement in many fields from bank notes and securities to the detection of pirate copies of, for example, drugs, compact discs or perfumes, and the authentication of valuable artifacts. In the case of bank notes and securities protection from forgery and counterfeiting is traditionally performed by the use of special papers, watermarks, embedded metal strips and intricate designs to make accurate copying or forgery as difficult as possible. Authentication of bank notes is then performed by visual inspection of printed designs and verification of the presence of watermarks and metal strips and possibly by inspection under ultraviolet light.

The protection of securities using magnetic inks is known from Japanese patent 58-86677, 24 May 1983, however such inks may also be replicated by a forger.

Another known method, disclosed in Japanese patent 57-62478, 15 April 1982, is based on the absorption and reflection of light in the visible and infrared spectra but the optical characteristics of documents change as they become worn or soiled resulting in false determinations of authenticity.

The incorporation of conducting strips into bank notes or credit cards and scanning by microwaves to generate a code to mark the document, for example by writing to a magnetic strip, and subsequently re-scanning the document and comparing the mark with the scan is also known from

WO 87/01845. However, it is possible for a forger to carry out the same procedure and thereby produce a document or card which is indistinguishable from a genuine article. In addition, the method taught in WO 87/01845 is dependent on the production and use of special materials and is not suitable for protecting existing documents.

The rapid development of high quality, relatively inexpensive, colour copying equipment could shortly lead to a loss of confidence in securities. In fact, in many countries people are already reluctant to use high denomination bank notes and other securities without repeated authentication. This could lead to a complete collapse in the monetary system and economic crisis.

Authentication is known as a branch of cryptography for verifying the source of encrypted messages via, for example, electronic signatures. In particular, the use of public key cryptosystems provides means not only of encrypting messages using public and secret keys, but also of authenticating the source of the message as discussed in *Welsh, D. Codes and Cryptography, Oxford, OUP, 1988, Ch. 12.*

The object of this invention is to provide a method for cost-effective authentication of a wide variety of articles without requiring special materials, which cannot be replicated by potential forgers or counterfeiters and which can be applied to existing articles and to apparatus for encoding articles for authentication.

Summary of Invention

According to a first aspect of this invention there is provided a method of authenticating articles using the steps of determining a distinguishing physical or

chemical characteristic of an article, encoding that physical or chemical characteristic, encrypting the encoded characteristic to form an encrypted representation, applying that encrypted representation to the article, subsequently authenticating the article by redetermining the physical or chemical characteristic, and reading and decrypting the encrypted representation to form a decrypted representation and comparing the decrypted representation of the recorded physical or chemical characteristic with the redetermined physical or chemical characteristic to determine the authenticity of the article.

In particular there is disclosed a method of authenticating articles wherein the physical or chemical characteristic is the micro-topography of an area of a surface of the article.

Advantageously, the micro-topography of an area of a surface of the article is scanned while the surface is illuminated from a single direction.

In an embodiment the micro-topography of an area of a surface of the article is scanned while the surface is illuminated from a first direction and subsequently re-scanned while the surface is sequentially illuminated from at least one further direction and the resultant images are combined to form the encoded characteristic.

In a particular embodiment the micro-topography of an area of a surface of the article is scanned while the surface is illuminated from a first direction and subsequently re-scanned while the surface is illuminated from a second direction, vectors are derived from the resultant two images and the vectors derived from one of the images are subtracted from the vectors derived from the other image to form the encoded characteristic.

BNSDOCID: <WO_9724699A1>

Depending on the nature of the article to be protected, the characteristic of the article encoded may be, for example:

Paper	micro-topography (reflection, transparency at different wavelengths, conductivity)
Metal	microstructure (reflection, transparency to different wavelengths, conductivity, crystalline structure)
Wood	microstructure (reflection, transparency to different wavelengths, conductivity)
Organic materials	nuclear magnetic resonance spectrum, electron paramagnetic resonance spectrum, infrared absorption
Living cells	DNA and/or RNA structure
Gaseous and liquid blends	nuclear magnetic resonance spectrum, electron paramagnetic resonance spectrum, infrared absorption
Crystals and gemstones	facets and edges, crystal lattice, nuclear quadrapole resonance
Optical storage media	irregularities of disc surface and thickness
Complex molecular structures	dispersion of optical rotation of optically active materials, spectrum of circular dichroism, spectrum of anomalous dispersion of X-rays,

individual spectrum of combinative dispersion, gas electronography, oscillatory infrared, electronic or ultraviolet spectrum

Preferably the encoding is encrypted and decrypted using a public key encryption system.

In a preferred embodiment the public key encryption system has a plurality of levels of security.

Advantageously additional characterising information is encoded together with the representation of the physical or chemical characteristic of the article.

In one application the article to be authenticated is a document such as a bank note or other security.

In another application the article is optical or magnetic information storage means preferably adapted so that information cannot be recovered from the storage means without authentication.

Preferably the area or portion of the article to be used in determining the physical or chemical characteristic is indicated by a plurality of reference marks.

Advantageously the encrypted coding marked on the article is formed from a plurality of marks such as dot or bar codes.

Preferably the article is a laser disk and the characteristic that is encoded is one of a representation of the topography of the disk, a representation of the topography of data on the disk, and a representation of topographical deviation of data on the disk from standardised topography of data, said characteristic

being encoded and encrypted to form said encrypted representation which is applied to the disk and the disk is subsequently authenticated by redetermining the encoded data and comparing the decrypted data with the redetermined data, so as to thereby determine the authenticity of the disk.

Advantageously if said comparison determines that the disk is authentic then a disk player is enabled to read information data on said disk but if said disk is not authenticated then said disk player is disabled and said disk will not "play".

According to a second aspect of this invention there is provided an apparatus for encoding articles for authentication including means for determining a distinguishing physical or chemical characteristic of an article, means for encoding that physical or chemical characteristic, means for encrypting said encoded characteristic as an encrypted representation and means for applying said encrypted representation to the article.

In one form of the apparatus, the physical or chemical characteristic encoded is the micro-topography of an area of a surface of the article.

Advantageously, scanning means are provided for scanning the micro-topography of an area of a surface of the article while the surface is illuminated from a first direction and subsequently re-scanning while the surface is sequentially illuminated from at least one further direction and means for combining the resultant images to form the encoded characteristic.

Advantageously, scanning means are provided for scanning the micro-topography of an area of a surface of the article while the surface is illuminated from a first direction and subsequently re-scanning while the surface is illuminated from a second direction, means for deriving vectors are derived from the resultant two images and subtracting means for subtracting the vectors derived from one of the images from the vectors derived from the other image to form the encoded characteristic.

Advantageously, the physical or chemical characteristic encoded is any one of nuclear magnetic resonance, nuclear quadrupole resonance spectrum, electron paramagnetic resonance spectrum, infrared absorption spectrum, optical rotation, DNA code, RNA code, circular dichroism spectrum, spectrum of anomalous dispersion of x-rays, individual combinative dispersion spectrum, gas electronography, oscillatory infrared, electronic or ultraviolet spectrum, the crystalline or lattice structure of the material constituting the article.

Preferably the encoded characteristic is encrypted and decrypted using a public key encryption system and advantageously the public key encryption system has a plurality of levels of security.

Preferably means are also provided for encoding additional characterising information together with the representation of the physical or chemical characteristic of the article.

In one form of the apparatus the article is a document such as a bank note or other security.

Preferably, means are provided for using reference marks so as to identify on the article the area or portion of

SUBSTITUTE SHEET (RULE 26)

the article to be used in determining the physical or chemical characteristic.

Advantageously, the representation of the encrypted coding marked on the article is formed from a plurality of dot or bar codes.

Conveniently, the apparatus further includes transporting means for orientating and moving an article successively relative to an analytical, measuring or scanning station, holding the article in or moving the article through said station while a physical or chemical characteristic of the article is determined, moving the article relative to a marking station, holding the article in or moving the article through said marking station while the article is marked and subsequently transporting the article out of the apparatus.

In an adaptation for authenticating documents, the apparatus includes transporting means for orientating and moving a document successively relative to a high resolution optical scanning station, for holding the article in or moving the article through said station while the micro-topography of an area of a surface of the document is determined, moving the document relative to a marking station, holding the document in or moving the article through said marking station while the document is marked and subsequently transporting the document out of the apparatus; said determining means is a means for scanning the micro-topography of a portion of a surface of said document; said means for encoding forms an encoded representation of the micro-topography; said means for encrypting said encoded representation uses at least one encryption key to form said encrypted representation, and said means for applying marks the encrypted representation on the document.

Preferably said means for determining a distinguishing physical or chemical characteristic of an article is a laser reader for reading one of the topography of a laser disk, the topography of information data on the disk, and a representation of topographical deviation of information data on the disk from standardised topography of data, said characteristic being encoded and encrypted to form said encrypted representation, and said means for applying said encrypted representation is a laser writer.

Advantageously when the characteristic that is encoded is the topographical deviation, comparator means is employed to determine an electrical signal representative of the deviation of the binary 0's and 1's from a standard depth for a 0 and 1.

According to a third aspect of this invention there is provided an apparatus for authenticating an article characterised in that the apparatus includes means for determining a physical or chemical characteristic of an article, means using one or more public decryption keys for decipering an encoded representation of that physical or chemical characteristic marked on the article, means for comparing the actual physical or chemical characteristic with the deciphered representation and means for indicating therefrom whether the article is authentic.

In a particular application, the determining means scans the micro-topography of the article and the comparing means compares the actual topography with the decoded representation.

Advantageously, said apparatus further includes secret decryption means, using for higher levels of security, the same secret encryption key to decrypt the

BNSDOCID: <WO_9724699A1>

representation as that used to encrypt the representation without disclosing said key to an operator.

Preferably the apparatus further includes error-correcting means to allow for changes in the chemical or physical characteristics subsequent to the encoding of the same, produced, for example, by wear, aging or soiling.

Advantageously the apparatus further includes transporting means for orientating and moving the article relative to an analytical, measuring or scanning station, holding the article in or moving the article through said station while a physical or chemical characteristic of the article is determined and subsequently transporting the article out of the apparatus.

In an adaptation for authenticating documents, the apparatus includes transporting means for orientating and moving a document relative to a high resolution scanning station, holding the article in or moving the article through said station while the micro-topography of a portion of a surface of the document is determined and subsequently transporting the article out of the apparatus; said determining means is a means for scanning the micro-topography of the document; means for reading and, using at least one decryption key, decrypting, an encrypted representation of the micro-topography previously marked on the document; means for comparing compares the encoded representation of the micro-topography so obtained with that determined by the apparatus.

Preferably said means for determining a distinguishing physical or chemical characteristic is a laser reader, said comparing means redetermines the encoded data and

compares the decrypted data with the redetermined data, and said indicating means is arranged to supply a signal to a disk player indicating authenticity of said disk whereby if said disk is judged not to be authentic the disk will not "play" and if it is judged to be authentic the disk will "play".

Preferably said means for determining a physical or chemical characteristic of an article is a laser reader and said means for comparing is a decision making means for comparing the deciphered representation with the actual characteristic that is read by said laser reader and said decision making means being adapted to enable or disable means for reading information data on said disk in dependence upon whether said disk is determined to be authentic or not.

According to a first feature of this invention there is provided a method of authenticating a laser disk such as a CD or CD-ROM using the steps of determining a characteristic of said disk that is one of a representation of the topography of the disk, a representation of the topography of data on the disk, and a representation of the topographical deviation of data on the disk from standardised topography of data, encoding the characteristic, encrypting the encoded characteristic to form an encrypted representation, applying the encrypted representation to the disk, subsequently authenticating the disk by redetermining the characteristic, and reading and decrypting the encrypted representation to form a decrypted representation, and comparing the decrypted representation of the recorded characteristic with the redetermined physical characteristic so as to thereby determine the authenticity of the disk.

Preferably if said comparison determines that the disk is authentic then a disk player is enabled to read information data on said disk but if said disk is not authenticated then said disk player is disabled and said disk will not play said information data.

According to a second feature of this invention there is provided an apparatus for encoding laser disks such as CDs or CD-ROMs including a laser reader for reading one of the topography of the disk, the topography of information data on the disk, and a representation of topographical deviation of information data on the disk from standardised topography of data, means for encoding the physical characteristic as an encoded characteristic, means for encrypting said encoded characteristic as an encrypted representation, and means for applying said encrypted representation to the article.

According to a third feature of this invention there is provided an apparatus for authenticating a laser disk such as a CD or CD-ROM including means for determining a physical characteristic of the disk by using laser reading means to read one of the topography of the disk, the topography of information data on the disk, and a representation of topographical deviation of information data on the disk from standardised topography of data, means using one or more public decryption keys for deciphering an encoded representation of that physical characteristic marked on the disk, means for comparing the actual physical characteristic with the deciphered representation, and means for authenticating said disk.

Reference to articles should be understood to include their associated packaging and labelling, particularly in relation to the determination of physical or chemical characteristics and in relation to marking with an encrypted representation.

Bri f description of drawings

The invention will now be described by way of example with reference to the accompanying drawings, in which:

Figure 1 shows a USA one hundred dollar bank note having a mark used to define a scanning area,

Figure 2 shows a USA one dollar bank note in which an encrypted representation is printed in accordance with an aspect of this present invention,

Figure 3 is a diagrammatic representation of the micro-topography of the scanned bank note paper,

Figure 4 is a diagrammatic view of the encrypted representation,

Figure 5 shows a micrograph of the surface structure illuminated from a right hand side direction,

Figure 6 shows a micrograph of the surface structure illuminated from a left hand side direction,

Figure 7 is a depiction of the resultant surface derived from the micrographs in Figures 5 and 6 for a clean bank note,

Figure 8 shows an encrypted representation derived from and applied to a clean bank note,

Figure 9 is a graphical representation of the correlation between the scanned surface and the deciphered encrypted representation for a clean bank note,

Figure 10 shows a depiction of the same area as Figure 7 after the surface has been damaged by wear and soiling,

Figure 11 shows an encrypted representation as in Figure 8 but after the surface has been damaged by wear and soiling,

Figure 12 is a graphical representation of the correlation between the deciphered encrypted representation and the re-scanned image for the worn and soiled surface, [please confirm]

Figure 13 is a block schematic diagram of the encoding apparatus,

Figure 14 is a block schematic diagram of the signal processing of the encoding apparatus,

Figure 15 is a block schematic diagram of the deciphering apparatus,

Figure 16 is a block schematic diagram of the signal processing performed by the deciphering apparatus,

Figure 17 is a block schematic of another embodiment of an encoding apparatus particularly useful with a laser disk, and

Figure 18 is a block schematic diagram of the deciphering and comparison apparatus to be used with the Figure 17 embodiment.

In the Figures like reference numerals denote like parts.

Preferred Embodiments of the Invention

The first embodiment is for the protection of paper money and securities from forgery by high resolution digital scanning a predetermined small (say 1 square millimetre) area of the micro-topography of the paper from which the

money or security is made and then printing on the paper an encrypted mark representing that topography.

As illustrated in Figure 1, a bank note 1, has a scanning area indicated by some pre-printed mark 2 on the paper; the mark 2 may be used by both the encoding and the authenticating apparatus to locate the precise area to be scanned for encoding and authenticating. Alternatively the deciphering apparatus may detect the location of the encrypted mark and from that position determine the area of paper to be topographically scanned.

An encrypted representation 3 is shown on a bank note 4 in Figure 2.

To understand how the encrypted mark or representation is derived, consider a microstructure represented diagrammatically by Figure 3, in which fibres 7 of the paper are shown as dark strands across a light background 8 of the paper matrix. The scanned area is partitioned by the scanner by the imposition of a grid defined by two orthogonal subdivided groups of reference lines 9, 10 in the y and x direction respectively at a resolution of 10 elements per millimetre square. Scanning along each line 10 of the grid so formed, using a suitable threshold value, each element is read as light or dark. These readings are digitised for x-axis elements 10a to give a digital reading of 0100110011 where 1 represents dark areas and 0 represents light areas, reading from left to right. The decimal equivalent of this binary number is 307 and the topography along this reading line may therefore be depicted by 307.

For this number to be encrypted and deciphered by an RSA public encryption system as described in *Rivest, R.L., Shamir, A. & Adleman, L. A method of obtaining digital signatures and public key cryptosystems. Comm. ACM 21,*

1978, pp 120-6 it is necessary for the operation by a secret key d to be reversible by a public key e to recover the decrypted value.

i.e. if the encrypted

$$C = M^d \bmod N$$

and the decrypted

$$M = C^e \bmod N$$

then substituting for C

$$M = [M^d]^e \bmod N$$

where C is the encrypted number
M is the number before encryption and after decryption
d is the (secret) encrypting key
e is the (public) decrypting key
mod N means that the modulus of the number it qualifies is taken i.e. the remainder after dividing by N

Now, as discussed in, for example, *Beckett, B. Introduction to Cryptology, Blackwell, 1988, Ch. 7* two numbers are said to be relatively prime if they have no common prime factors (other than 1) and the number of integers Φ relatively prime to a number n is given by the Euler totient function:

$$\Phi(n) = n[(1-1/p_1)(1-1/p_2) \ . \ . \ . \ (1-1/p_m)]$$

where p_i are the prime factors of n.

If n is the product of two prime numbers p, q then

$$\Phi(n) = n(1-1/p)(1-1/q)$$
$$= \frac{pq(p-1)(q-1)}{pq}$$
$$= (p-1)(q-1)$$

Now it is known that the required relationship:

$$M = [M^d]^e \bmod N$$

is equivalent to (see *Beckett, B. Introduction to Cryptology, Blackwell, 1988, Ch. 9*)

$$M = M^{de \bmod \Phi(n)} \bmod N$$

which is satisfied by

$$de \bmod \Phi(n) = 1 \quad [\text{for } M<N]$$

i.e. we seek values of d which when multiplied by e and divided into $\Phi(n)$ leave a remainder of 1.

For the purposes of illustration, let n = N and be the product of the primes p=17, q=31 and choose key e=7

Then $N = pq = 527$

$\Phi(N) = (p-1)(q-1) = 480$

Then we need to find a value of d such that

$$7d \bmod 480 = 1$$

By evaluation, this is satisfied by d = 343
(since then 7d = 2401, 2401/480 = 5 + r1)

Therefore to encrypt the scanned value M=307 we need to calculate:

$$C = M^d \bmod N$$

$$= 307^{343} \bmod 527$$

$$= 307^{101010111} \bmod 527 \quad \text{(expressed in binary)}$$

But $101010111 = 2^8 + 2^6 + 2^4 + 2^2 + 2^1 + 2^0$

Therefore

$$C = 307^{(256+64+16+4+2+1)} \bmod 527$$

$$= (307^{256} * 307^{64} * 307^{16} * 307^4 * 307^2 * 307) \bmod 527$$

But it can be shown that

$$307^2 \bmod 527 = 443 \bmod 527$$
$$307^4 \bmod 527 = 205 \bmod 527$$
$$307^8 \bmod 527 = 392 \bmod 527$$
$$307^{16} \bmod 527 = 307 \bmod 527$$
$$307^{32} \bmod 527 = 443 \bmod 527$$
$$307^{64} \bmod 527 = 205 \bmod 527$$
$$307^{128} \bmod 527 = 392 \bmod 527$$
$$307^{256} \bmod 527 = 307 \bmod 527$$

Therefore

$$C = 307*205*307*205*443*307 \bmod 527$$

substituting again $307*307=443$ and $205*205 = (307^4)^2 = 392$ for ease of calculation:

$$C = 443*392*443*307 \bmod 527$$
$$= 23,617,389,656 \bmod 527$$
$$= 69$$
$$= 1000101 \text{ in binary}$$

Therefore the value 0100110011 (307) which is the encoded characteristic of the topography is encrypted as 1000101 (69).

To form a representation of this encrypted value it may be expressed as a bar code printed onto the bank note, as shown in Figure 4, in which a bar 16 represents the value 1 and the absence of a bar represents a value 0. For the purpose of illustration and clarification only, the binary values 7 are also printed alongside the bar code in Figure 4. Each reading line scanned will then result in a similar bar code which may be printed as a series of bar codes.

To check the authenticity of the bank note the recipient needs to retrieve the original value 307 from the encrypted value 69 using the published key e = 7 and the published modulus mod(527).

Using

$$M = C^e \bmod(N)$$
$$= 69^7 \bmod(527)$$
$$= 69^4 * 69^2 * 69 \bmod(527)$$
$$= 324 * 18 * 69 \bmod(527)$$
$$= 307$$

In this example a small value of N has been selected for ease of demonstration. In an actual embodiment a large value of N would be used. Where N is more than 10^{300} it is practically infeasible to determine the secret key from the published information.

In a preferred version of this embodiment multiple levels of security are incorporated using higher values of mod N for the higher levels of security, because prime factorisation becomes computationally infeasible as N increases in size. However, the use of high values of N involves increased processing costs so that retailers may, for example, be equipped with apparatus to read the lowest level security coding, high street banks with higher level security apparatus and the issuing bank with

the highest level, which may include only secret keys and no public keys.

In a practical embodiment it is necessary to select a physical characteristic of the article being protected which cannot be duplicated by a potential forger and if, for example, a surface is scanned using illumination from only one direction, then a scanner of sufficiently high resolution must be used that details of the topography may be resolved which cannot be replicated by any known technique.

In a second embodiment bank notes are protected by digitally combining the images of the micro-topography scanned when sequentially illuminated from two or more directions. Figure 5 shows the surface of a bank note illuminated from a right hand side direction and Figure 6 shows the bank note illuminated from a left hand side direction. Preferably an un-printed area of the bank note is scanned to reduce the effect of features common to all notes printed alike.

Using an optical scanner the first image shown in Figure 5 is read and represented by $X=(x_1, x_2, \ldots x_n)$ which is digitised and then the second image, shown in Figure 6, is read and represented by $Y=(y_1, y_2, \ldots y_n)$ which is also digitised. These digitised representations are combined, e.g. by subtraction ($L = X-Y$), into a composite image $L=(l_1, l_2, \ldots l_n)$ to provide an enhanced representation of the micro-topography as illustrated in pictorial form in Figure 7. In a preferred embodiment the scanned bit maps are vectorised into vectors L. Using such a combined image reduces the possibility of fraudulent reproduction of the image while distinguishing between topography and surface markings.

Using any suitable known redundancy reduction algorithm the vectors L of size n are transformed into vectors L* of considerably smaller size (n*) than L. In practice n* may be of the order of 900 where n is of the order of 10^4. Ideally this reduction in redundancy increases the efficiency of the encrypting algorithm.

In a preferred embodiment the vector L* may be combined with a coded sequence Z representing additional information such as the denomination of the bank note, and/or the date and time of issue etc., to obtain the vector M.

Using any public key cryptosystem or electronic signature algorithm the unencrypted vector M is encrypted to produce the cryptotext C.

Preferably, to allow for error correction to accommodate changes in the micro-topography from wear or soiling etc., the encrypted code C is transferred to an error correction code C*. The size of C* will depend on the level of error correction required. (The size of C* will be between 2000 and 10000 to correct 200 to 2000 errors (see Reddy S.M., Robinson J.P., Random error and burst correction by iterated codes - IEEE Trans. Information Theory 1970, Vol.IT-16, p452-459 and Chien R.T. Cyclic decoding procedures for Bose-Chaudhuri-Hocquemghem codes - IEEE Trans. Information Theory 1964, Vol.IT-10, p357-363).

The resulting encrypted image is printed on an area of the bank note, preferably close to the area scanned, as shown in Figure 8. This encrypted representation is shown printed on a bank note in Figure 2. For the example shown, a linear cascade code with parameters (64.64=4096, 36.36=1296, 12x12=144) was used which corrects for a maximum of 71 errors (see the aforementioned IEEE Trans.

Information Theory) and the image was encrypted using the RSA public cryptosystem with modulus component $N=10^{310}$.

Information about the method of protection, the redundancy algorithms and encryption (except the encrypting key) may be published for interested parties such as banks and retailers, to enable them to authenticate the bank notes.

To authenticate the notes, similar procedures are performed to those carried out by the producer to perform encryption, but in addition, allowance must be made for differences introduced both in the scanned area of paper and in the printed encrypted image as a result of wear and soiling. The surface is scanned illuminated from one or more directions as before to derive an image $\hat{L}$. Similarly the printed encoded image is scanned to produce the image $\hat{C}$ (which differs from C* by the errors t*).

Using known error correcting algorithms (see the aforementioned IEEE Trans. Information Theory) it is possible to correct for the t* errors to obtain the original encrypted image C* (unless t* is greater than the design maximum of errors t).

Using published information about the encryption algorithm and the public decryption key e, the unencrypted description M is obtained, from which the vectors Z and L* are recovered. From L*, using error correction procedures, the starting vector L is determined.

The correlation between L and $\hat{L}$ is calculated (as represented graphically in Figure 9) and from the correlation coefficient, a decision can be made on the authenticity of the bank note.

The success with which the method accommodates wear and soiling of the bank notes is illustrated by Figures 10, 11 and 12 which relate to soiled notes and correspond to Figures 7, 8 and 9 respectively for clean notes. It can be seen that the correlation between the micro-topography and the decoded encrypted for soiled notes is substantially as good as that for unsoiled notes.

An embodiment of the encryption apparatus will now be described with reference to Figure 13 in which a mechanical transportation device 130 appropriately aligns and orients a bank note (not shown) and moves the bank note to a scanning station 131 having a read head 132, and holds it stationary in, or incrementally or continuously transports it through, the scanning reading station 131 as required for the scanning device to produce an image of the predetermined area of the note. Digital signals X and Y, representing images of the micro-topography illuminated from two different directions, are passed via a respective one of lines 133 from the scanning station to digital processing unit 134 where the addition of further information, redundancy reduction, conversion to error correcting code and encryption are performed.

The bank note is moved by the transport device 130 to a printing station 135, and held stationary there or transported therethrough for print head 136 to print on a predetermined portion of the note using processed and encrypted signals C* over line 136 from the data processing unit 134. Another outlet 137 from the processor 134 outputs parameter signals such as the value of the public key and the modulus number to be used for subsequently authenticating the bank note.

The manner of operation of the encryption processor 11 will now be described with reference to the block diagram Figure 14.

The processor 134 unit has inputs via lines 133 from the scanner along which pass signals representing the images X and Y into an arithmetic unit 140 where they are combined to form a derived image L=Y-X. Output from the arithmetic unit 140 is fed to a redundancy reduction unit 141, the output from which is fed to a combiner 142, a second input of which is derived from a storage or input device 143 which holds and adds additional information Z such as denomination, date of issue etc. about the bank note being encoded, to form the image M=L+Z. Output from the combiner 142 is input to an encryption device 144 which also has an input from a key generating unit 145. A second output from the key (d) generating block forms one of the outputs 137 of the processor 134. The output of the encryption device ($C=M^d \bmod N$) formed from M and the encryption key d passes to the error correction coding unit 146 the outlet of which passes the image C* to form the output 136 of the processor.

An embodiment of the authenticating apparatus will now be described with reference to Figure 15 in which a mechanical transporting device 150 correctly aligns and orients a bank note and moves the bank note to or through a scanning station 151 having a read head 152. Output signals corresponding to images $\hat{X}$ and $\hat{Y}$, from scanning the micro-topography of the bank note illuminated from two directions are input via lines 153 to an authenticating processor 154. Additionally, an output signal from reading the encrypted representation $\hat{C}$ is passed via line 155 from the scanner to the processor 154. Output from the digital processing unit on the authenticity of the bank note is passed via line 156 to a display unit 157 and additional information Z on for

example the encoded denomination of the note is passed to the display unit 157 via a line 158. The open key e and numbers N are input to the processor 154 via line 159.

An embodiment of the authenticating processor 154 will now be described with reference to Figure 16 in which output signals corresponding to images $\hat{X}$ and $\hat{Y}$, from scanning the micro-topography of the bank note illuminated from two directions are input via lines 153 to the arithmetic unit 160 where $\hat{L} = \hat{Y}-\hat{X}$ is calculated, and the output is input to a correlator 161. Output on line 155 from the scanning station, representing a scan of the encrypted printed image $\hat{C}$, is input to a decoder 162 which performs error correction and outputs $C^* = Z+M$ to a decrypting unit 163 which deciphers M and Z using the open key e and modulus N entered via the input 159 corresponding to the output from outlet 137. The decrypting unit 163 then passes the additional information Z to the line 158 and passes L^* to an unpacking unit 164 where redundancy is restored to reproduce L. The unpacking unit 164 passes L to the correlator 161 where the correlation coefficient between L and $\hat{L}$ is calculated which is then passed to a decision-making unit 165 where a decision on authenticity is made and passed via line 156 to the information display unit 157.

It is currently envisaged that the invention will also have practical importance with laser read disks, such as CD-ROMs. The characteristic that is encoded may be representative of the topography of the disk or of the topography of the data on the disk. The data on a laser disk is in binary form and representations of 0's and 1's are given by different topographical heights or depths of groove within the disk. In an ideal disk 0's will be at one standardised depth and 1's will be at another standardised depth. However, in a practical disk there

is deviation from the standard. The present invention preferably, alternatively, determines the deviation from the standard and encodes the deviation for application after encryption to the disk for subsequent authentication purposes.

Referring to Figure 17, a laser disk 170 has the binary information thereon read by a laser reader 171 to provide encoded information X. The encoded information X is representative of the actual depth of the binary data and this is compared with a standardised binary depth 0 or 1 in a comparator to provide X information that is fed to a processor 173. The processor, in similar manner to the processor 134, provides C* data 138 which is fed to a laser writer 174. The laser writer then applies the encrypted representation onto, for example a track, on the disk 170.

So as to authenticate the disk 170, it is read by a laser reader 181 which provides $\hat{C}$ and X information to a processor 182 which is similar to the processor 154. The processor 182 outputs a signal M representative of the original unencrypted message on line 156. The signal M is applied to a decision making circuit 183 which is similar to the decision making element 165. The decision making circuit 183 determines if the signal that is read from the laser disk is valid and if it is not then the decision making circuit 183 will send a signal to the standard circuitry of the laser disk player not to play the disk, or if it is valid, to permit the disk to be played.

In such a manner laser disks can be checked for authenticity.

It will therefore be understood that in the present invention a physical or chemical characteristic of the material of an article is determined, the characteristic is encoded, and the encoded characteristic is encrypted using a secret key. The encrypted representation is then applied to the article. The article is subsequently authenticated by re-determining the physical or chemical characteristic and reading and decrypting, using a public key or keys, the encrypted representation. The decrypted representation is compared with the redetermined physical or chemical characteristic to determine the authenticity of the article.

It will now also be understood that in the present invention the fact that the authentication code is derived from the nature of the material of the article, merely having encoding means that duplicating the code is of no avail to the potential forger, unless the forger can also duplicate the physical characteristic encoded, which can be made infeasible by an appropriate choice of characteristic and the resolution at which it is determined. For example, the topographic structure of each and every note will be different in the small area that is predeterminedly scanned. Further, the use of a suitable encryption system makes it practically infeasible for a forger to duplicate the process and mark the document or product himself. Therefore, by redetermining the physical characteristic and comparing it with the mark which he has deciphered with a public key, the recipient is able to distinguish between genuine and forged articles.

CLAIMS

1. A method of authenticating articles using the steps of determining a distinguishing physical or chemical characteristic of an article, encoding that physical or chemical characteristic, encrypting the encoded characteristic to form an encrypted representation, applying that encrypted representation to the article, subsequently authenticating the article by redetermining the physical or chemical characteristic, and reading and decrypting the encrypted representation to form a decrypted representation and comparing the decrypted representation of the recorded physical or chemical characteristic with the redetermined physical or chemical characteristic to determine the authenticity of the article.

2. A method of authenticating articles as claimed in claim 1 wherein the physical or chemical characteristic is the micro-topography of an area of a surface of the article.

3. A method of authenticating articles as claimed in claim 1 or 2 wherein the micro-topography of an area of a surface of the article is scanned while the surface is illuminated from a single direction.

4. A method of authenticating articles as claimed in claim 2 wherein the micro-topography of an area of a surface of the article is scanned while the surface is illuminated from a first direction and subsequently re-scanned while the surface is sequentially illuminated from at least one further direction and the resultant images are combined to form the encoded characteristic.

5. A method of authenticating articles as claimed in claim 2 wherein the micro-topography of an area of a

surface of the article is scanned while the surface is illuminated from a first direction and subsequently re-scanned while the surface is illuminated from a second direction, vectors are derived from the resultant two images and the vectors derived from one of the images are subtracted from the vectors derived from the other image to form the encoded characteristic.

6. A method of authenticating articles as claimed in claim 1 wherein the physical or chemical characteristic is the nuclear magnetic resonance spectrum of material constituting the article.

7. A method of authenticating articles as claimed in claim 1 wherein the physical or chemical characteristic is the nuclear quadrupole resonance spectrum of material constituting the article.

8. A method of authenticating articles as claimed in claim 1 wherein the physical or chemical characteristic is the electron paramagnetic resonance spectrum of material constituting the article.

9. A method of authenticating articles as claimed in claim 1 wherein the physical or chemical characteristic is the infrared absorbtion spectrum of material constituting the article.

10. A method of authenticating articles as claimed in claim 1 wherein the physical or chemical characteristic is the dispersion of optical rotation of optically active material which is a constituent of the article.

11. A method of authenticating articles as claimed in claim 1 wherein the physical or chemical characteristic encoded is the DNA code of material constituting the article.

12. A method of authenticating articles as claimed in claim 1 wherein the physical or chemical characteristic encoded is the RNA code of material constituting the article.

13. A method of authenticating articles as claimed in claim 1 wherein the physical characteristic encoded is any one of circular dichroism spectrum, spectrum of anomalous dispersion of x-rays, individual combinative dispersion spectrum, gas electronography, oscillatory infrared, electronic or ultraviolet spectrum, the crystalline or lattice structure of material constituting the article.

14. A method of authenticating articles as claimed in any of the preceding claims wherein the encoding is encrypted and decrypted using a public key encryption system.

15. A method of authenticating articles as claimed in claim 14 wherein the public key encryption system has a plurality of levels of security.

16. A method of authenticating articles as in any of the preceding claims wherein additional characterising information is encoded together with the representation of the physical or chemical characteristic of the article.

17. A method of authenticating articles as claimed in any of the preceding claims wherein the article is a document such as a bank note or other security.

18. A method of authenticating articles as claimed in any of claims 1-16 wherein the article is an optical or magnetic information storage means adapted so that

information cannot be recovered from the storage means without authentication.

19. A method for authenticating articles as in any of the preceding claims wherein the area or portion of the article to be used in determining the physical or chemical characteristic is indicated by a plurality of reference marks.

20. A method of authenticating articles as in any of the preceding claims wherein the representations of the encrypted coding marked on the article is formed from a plurality of marks such as dot or bar codes.

21. A method of authenticating articles as in claim 1 wherein the article is a laser disk and the characteristic that is encoded is one of a representation of the topography of the disk, a representation of the topography of data on the disk, and a representation of topographical deviation of data on the disk from standardised topography of data, said characteristic being encoded and encrypted to form said encrypted representation which is applied to the disk and the disk is subsequently authenticated by redetermining the encoded data and comparing the decrypted data with the redetermined data, so as to thereby determine the authenticity of the disk.

22. A method of authenticating an article as claimed in claim 21 wherein if said comparison determines that the disk is authentic then a disk player is enabled to read information data on said disk but if said disk is not authenticated then said disk player is disabled and said disk will not "play".

23. An apparatus for encoding articles for authentication including means (132) for determining a

distinguishing physical or chemical characteristic of an article, means (134) for encoding that physical or chemical characteristic, means (134) for encrypting said encoded characteristic as an encrypted representation, and means (136) for applying said encrypted representation to the article.

24. An apparatus for encoding articles for authentication as claimed in claim 23, wherein the physical or chemical characteristic encoded is the micro-topography of an area of a surface of the article.

25. An apparatus for encoding articles for authentication as claimed in claim 24, wherein scanning means (132) are provided for scanning the micro-topography of an area of a surface of the article while the surface is illuminated from a first direction and subsequently re-scanning while the surface is sequentially illuminated from at least one further direction and means for combining the resultant images to form the encoded characteristic.

26. An apparatus for encoding articles for authentication as claimed in claim 25, wherein scanning means (132) are provided for scanning the micro-topography of an area of a surface of the article while the surface is illuminated from a first direction and subsequently re-scanning while the surface is illuminated from a second direction, means for deriving vectors are derived from the resultant two images and subtracting means (140) for subtracting the vectors derived from one of the images from the vectors derived from the other image to form the encoded characteristic.

27. An apparatus for encoding articles for authentication as claimed in claim 23, wherein the physical or chemical characteristic encoded is any one of

nuclear magnetic resonance, nuclear quadrupole resonance spectrum, electron paramagnetic resonance spectrum, infrared absorption spectrum, dispersion of optical rotation, DNA code, RNA code, circular dichroism spectrum, spectrum of anomalous dispersion of x-rays, individual combinative dispersion spectrum, gas electronography, oscillatory infrared, electronic or ultraviolet spectrum, and the crystalline structure of the material of the article.

28. An apparatus for encoding articles for authentication as claimed in any of the claims 23-27 wherein the encoded characteristic is encrypted and decrypted using a public key encryption system.

29. An apparatus for encoding articles for authentication as claimed in claim 28, wherein the public key encryption system has a plurality of levels of security.

30. An apparatus for encoding articles for authentication as claimed in any of the claims 23-29, wherein means (142, 143) are provided for encoding additional characterising information together with the representation of the physical or chemical characteristic of the article.

31. An apparatus for encoding articles for authentication as claimed in any of the claims 23-30, wherein the article is a document such as a bank note (1,4) or other security.

32. An apparatus for encoding articles for authentication as claimed in any of the claims 23-31, wherein means are provided for using reference marks (2) so as to identify on the article the area or portion of

the article to be used in determining the physical or chemical characteristic.

33. An apparatus for encoding articles for authentication as claimed in any of the claims 23-32, wherein the representation of the encrypted coding marked on the article is formed from a plurality of dot or bar codes (16).

34. An apparatus as claimed in any of claims 23-33 further including transporting means (130) for orientating and moving an article successively relative to an analytical, measuring or scanning station, holding the article in or moving the article through said station while a physical or chemical characteristic of the article is determined, moving the article relative to a marking station, holding the article in or moving the article through said marking station while the article is marked and subsequently transporting the article out of the apparatus.

35. An apparatus as claimed in claims 23-33 further including transporting means (130) for orientating and moving a document successively relative to a high resolution optical scanning station, for holding the article in or moving the article through said station while the micro-topography of an area of a surface of the document is determined, moving the document relative to a marking station, holding the document in or moving the article through said marking station while the document is marked and subsequently transporting the document out of the apparatus; said determining means (132) is a means for scanning the micro-topography of a portion of a surface of said document; said means for encoding (134) forms a encoded characteristic of the micro-topography; said means (134) for encrypting said encoded characteristic uses at least one encryption key to form

said encrypted representation, and said means (136) for applying marks the encrypted representation on the document.

36. An apparatus as claimed in claim 23 wherein said means for determining a distinguishing physical or chemical characteristic of an article is a laser reader (171) for reading one of the topography of a laser disk, the topography of information data on the disk, and a representation of topographical deviation of information data on the disk from standardised topography of data, said characteristic being encoded and encrypted to form said encrypted representation, and said means for applying said encrypted representation is a laser writer (174).

37. An apparatus for encoding articles as claimed in claim 36 wherein, when the characteristic that is encoded is the topographical deviation, comparator means (172) is employed to determine an electrical signal representative of the deviation of the binary 0's and 1's from a standard depth for a 0 and 1.

38. An apparatus for authenticating an article characterised in that the apparatus including means (152) for determining a physical or chemical characteristic of an article, means (154) using one or more public decryption keys for deciphering an encoded representation of that physical or chemical characteristic marked on the article, means (161, 165) for comparing the actual physical or chemical characteristic with the deciphered representation, and means (157) for indicating therefrom whether the article is authentic.

39. An apparatus as claimed in claim 38 wherein the determining means (152) scans the micro-topography of the

article and the comparing means (161, 165) compares the actual topography with the decoded representation.

40. An apparatus as claimed in claims 38 or 39 further including secret decryption means (163) using, for higher levels of security, the same secret encryption key to decrypt the representation as that used to encrypt the representation without disclosing said key to an operator.

41. An apparatus as claimed in claims 38-40 further including error-correcting means (146) to allow for changes in the chemical or physical characteristics subsequent to the encoding of the same, produced, for example, by wear, aging or soiling.

42. An apparatus as claimed in any of claims 38-41 further including transporting means (150) for orientating and moving the article relative to an analytical, measuring or scanning station, holding the article in or moving the article through said station while a physical or chemical characteristic of the article is determined and subsequently transporting the article out of the apparatus.

43. An apparatus as claimed in any of claims 38-41 further including transporting means (150) for orientating and moving a document relative to a high resolution scanning station, holding the article in or moving the article through said station while the micro-topography of a portion of a surface of the document is determined and subsequently transporting the article out of the apparatus; sa[illegible] determining means (152) is a means for scanning the mi[illegible]-topography of the document; means (152, 162, 163) for [illegible]ading and, using at least one decryption key, decrypting, an encrypted representation of the micro-topography previously marked on the

document; and said means for comparing (161, 165) compares the encoded characteristic of micro-topography so obtained with that determined by the apparatus.

44. An apparatus as claimed in claim 38 wherein said means for determining a distinguishing physical or chemical characteristic is a laser reader (181), said comparing means (182) redetermines the encoded data and compares the decrypted data with the redetermined data, and said indicating means (157) is arranged to supply a signal to a disk player indicating authenticity of said disk whereby if said disk is judged not to be authentic the disk will not "play" and if it is judged to be authentic the disk will "play".

45. An apparatus as claimed in claim 38 wherein said means for determining a physical or chemical characteristic of an article is a laser reader (181) and said means for comparing is a decision making means (183) for comparing the deciphered representation with the actual characteristic that is read by said laser reader (181) and said decision making means (183) being adapted to enable or disable means for reading information data on said disk in dependence upon whether said disk is determined to be authentic or not.

46. A method of authenticating a laser disk such as a CD or CD-ROM using the steps of determining a characteristic of said disk that is one of a representation of the topography of the disk, a representation of the topography of data on the disk, and a representation of the topographical deviation of data on the disk from standardised topography of data, encoding the characteristic, encrypting the encoded characteristic to form an encrypted representation, applying the encrypted representation to the disk, subsequently authenticating the disk by redetermining the

characteristic, and reading and decrypting the encrypted representation to form a decrypted representation, and comparing the decrypted representation of the recorded characteristic with the redetermined physical characteristic so as to thereby determine the authenticity of the disk.

47. A method of authenticating a disk as claimed in claim 46, wherein if said comparison determines that the disk is authentic then a disk player is enabled to read information data on said disk but if said disk is not authenticated then said disk player is disabled and said disk will not play said information data.

48. An apparatus for encoding laser disks such as CDs or CD-ROMs including a laser reader (171) for reading one of the topography of the disk, the topography of information data on the disk, and a representation of topographical deviation of information data on the disk from standardised topography of data, means (173) for encoding the physical characteristic as an encoded characteristic, means (173) for encrypting said encoded characteristic as an encrypted representation, and means (174) for applying said encrypted representation to the article.

49. An apparatus for authenticating a laser disk such as a CD or CD-ROM including means for determining a physical characteristic of the disk by using laser reading means (181) to read one of the topography of the disk, the topography of information data on the disk, and a representation of topographical deviation of information data on the disk from standardised topography of data, means (182) using one or more public decryption keys for deciphering an encoded representation of that physical characteristic marked on the disk, means (182) for comparing the actual physical characteristic with the

deciphered representation, and means (183) for authenticating said disk.

BNSDOCID: <WO_9724699A1>

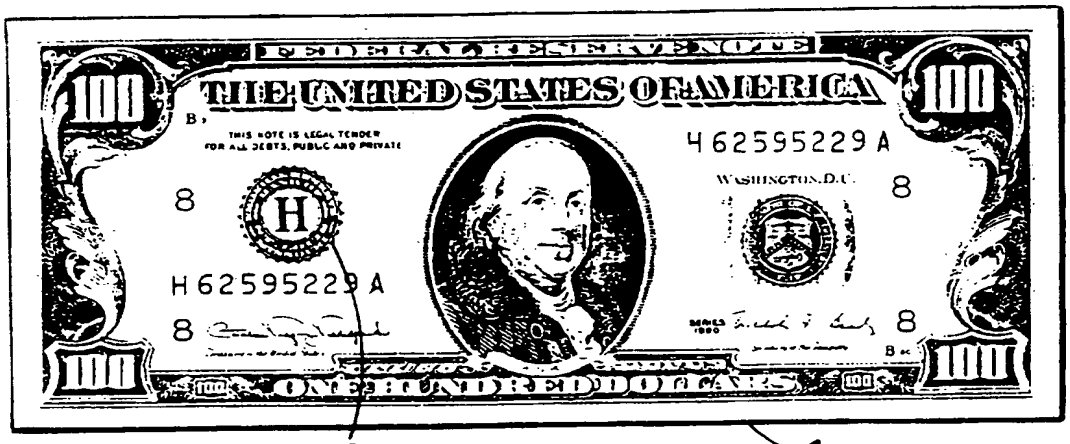


Fig. 1

Fig. 2

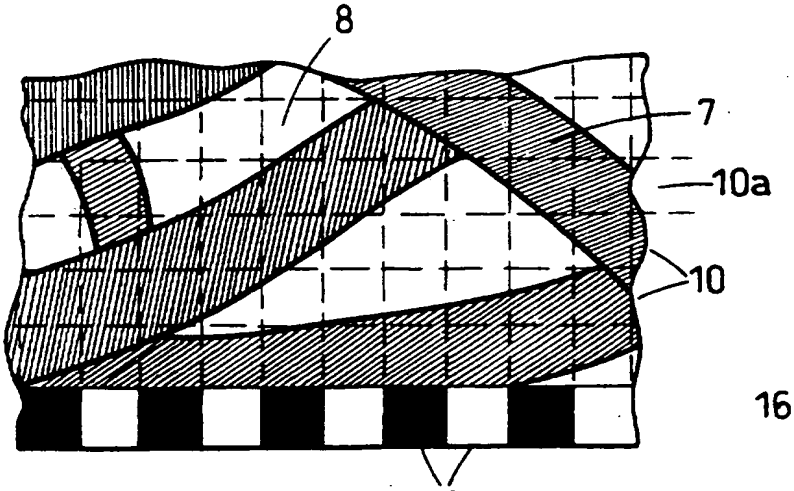


Fig. 3

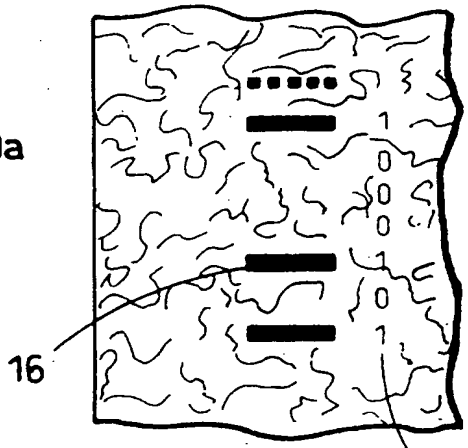


Fig. 4

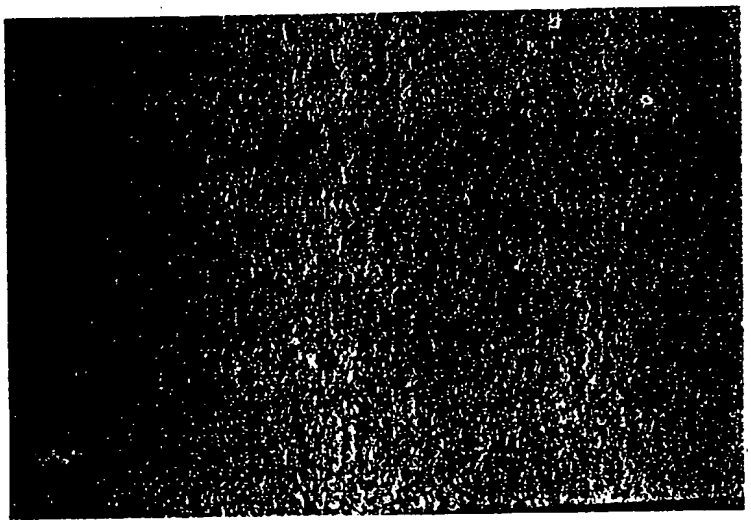


Fig. 5

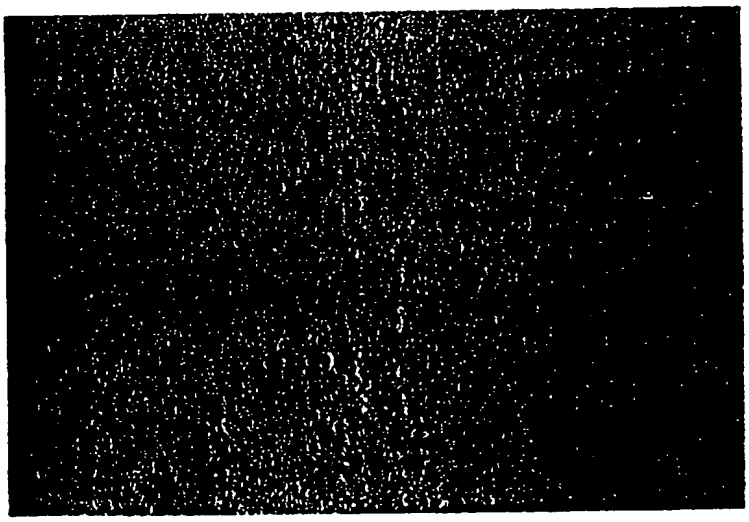


Fig. 6

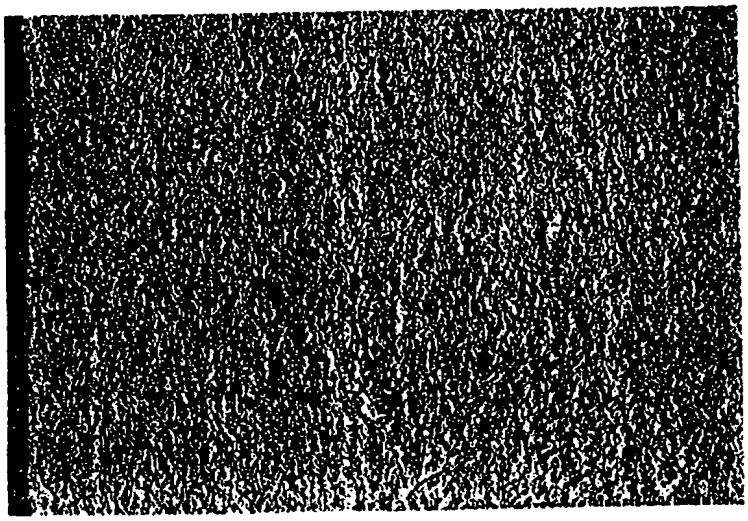


Fig. 7

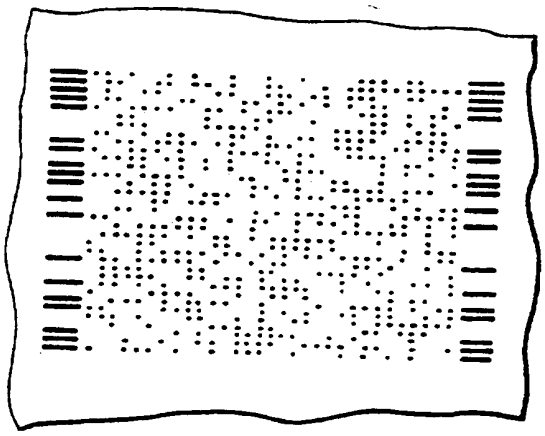


Fig. 8

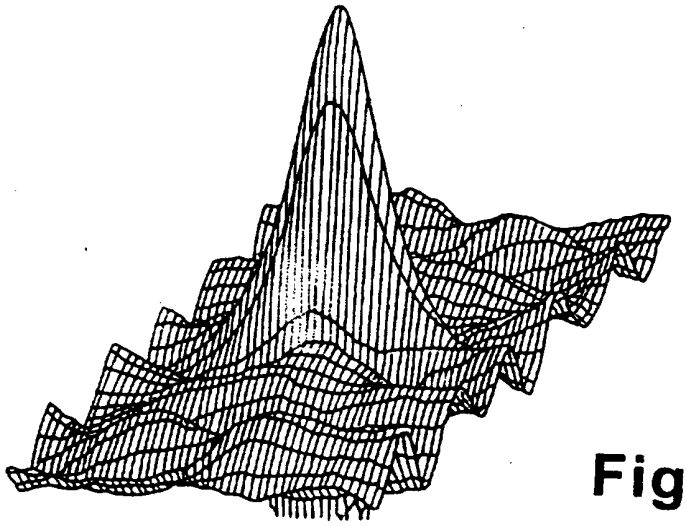


Fig. 9

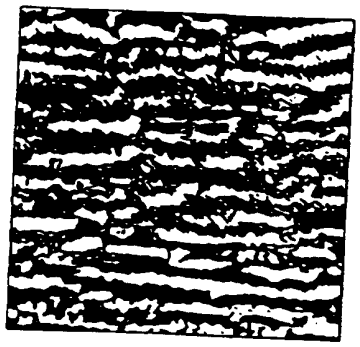


Fig. 10

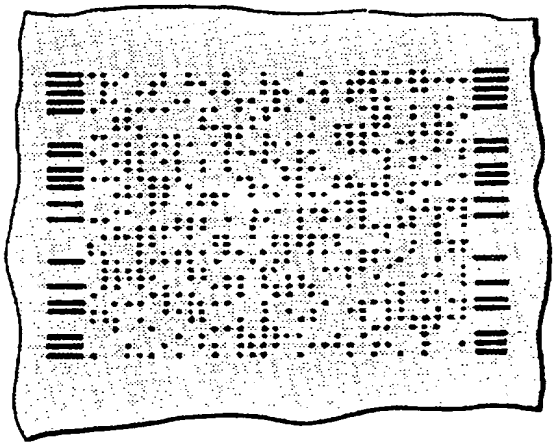


Fig. 11

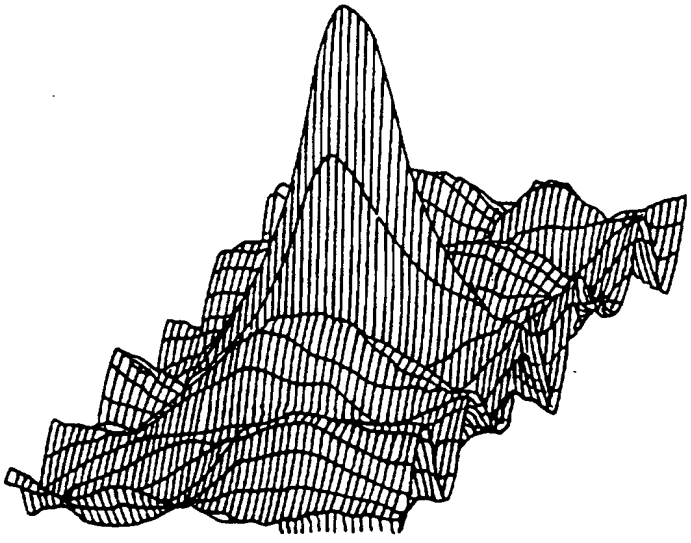


Fig. 12

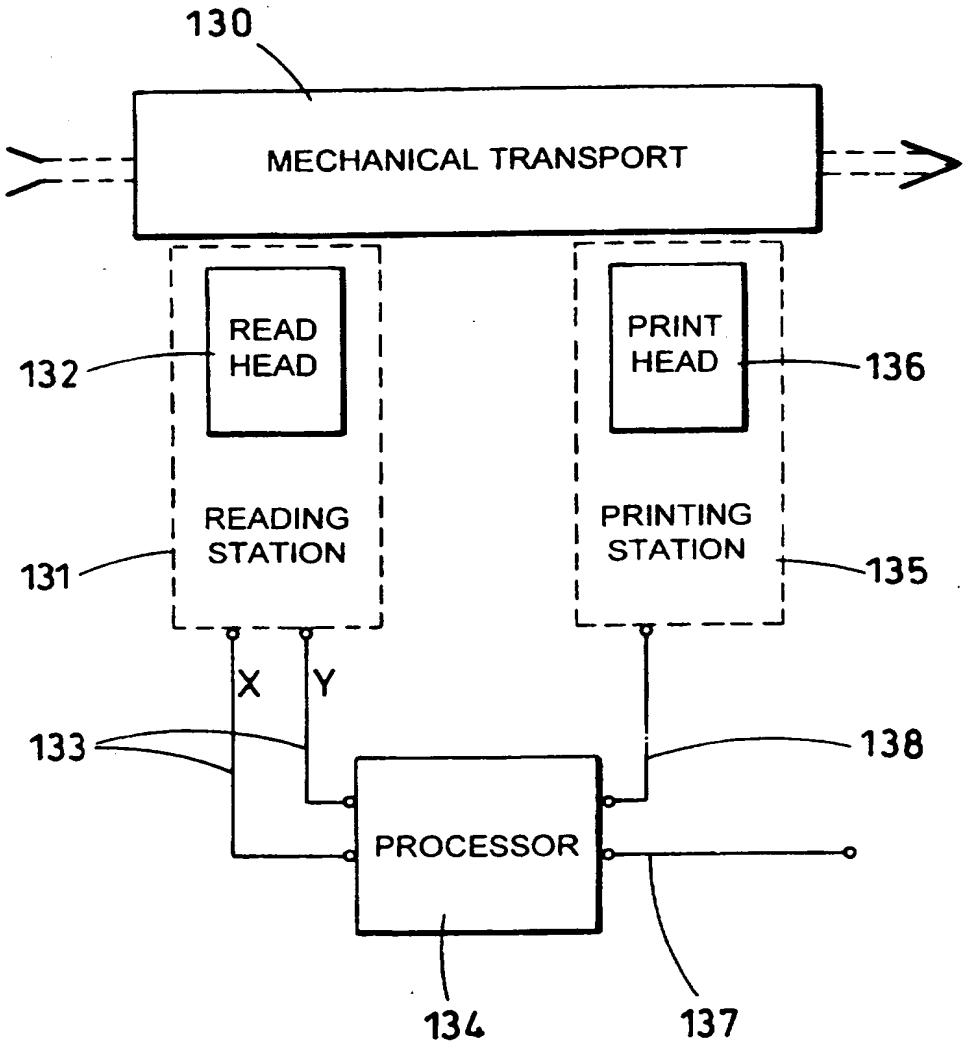

130
MECHANICAL TRANSPORT
READ HEAD
132
PRINT HEAD
136
READING STATION
131
PRINTING STATION
135
X
Y
133
138
PROCESSOR
134
137

Fig. 13

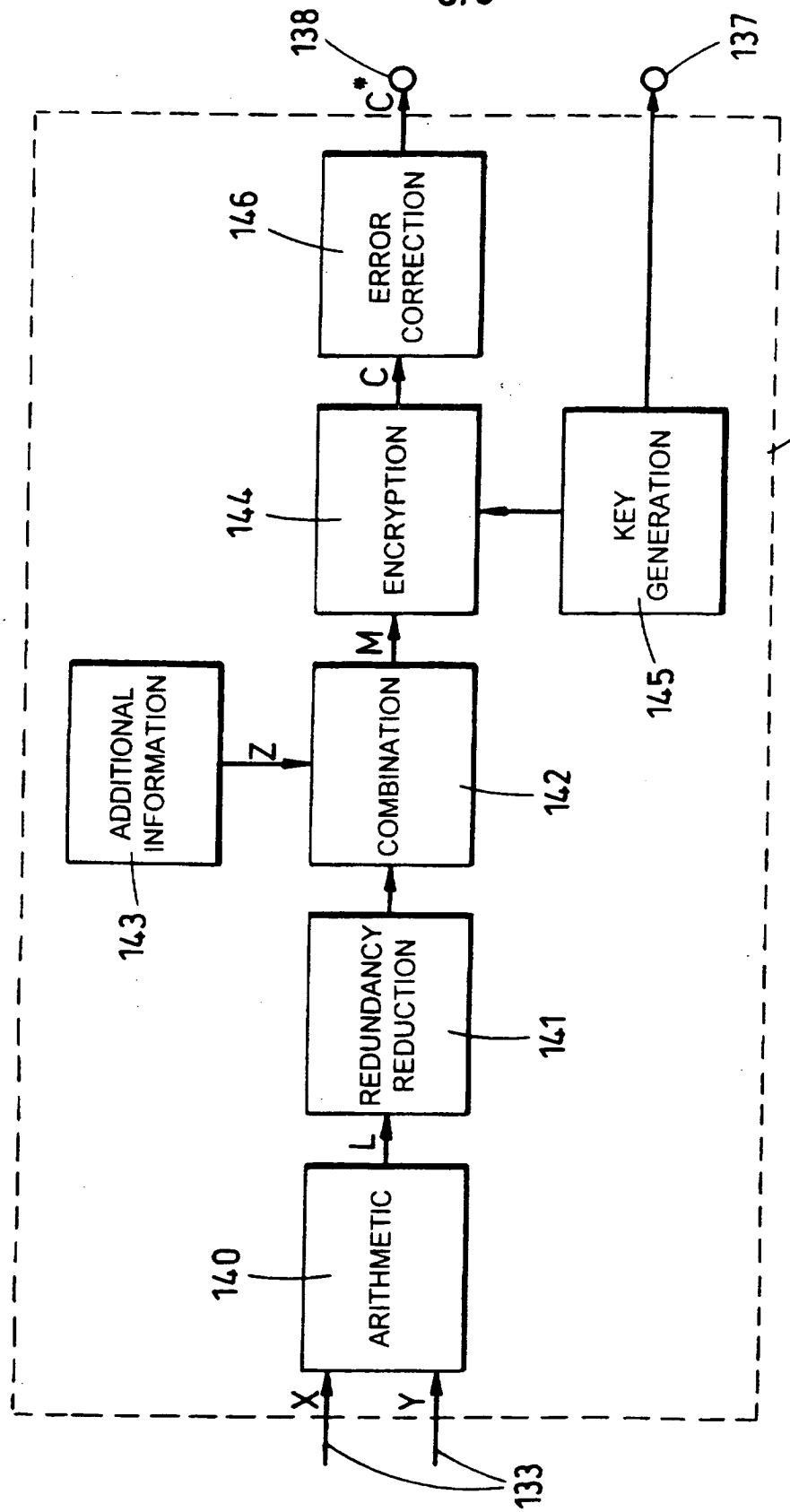

138
IC*
137
146
ERROR CORRECTION
C
144
ENCRYPTION
KEY GENERATION
134
M
ADDITIONAL INFORMATION
Z
COMBINATION
142
145
143
REDUNDANCY REDUCTION
141
L
140
ARITHMETIC
X
Y
133

Fig. 14

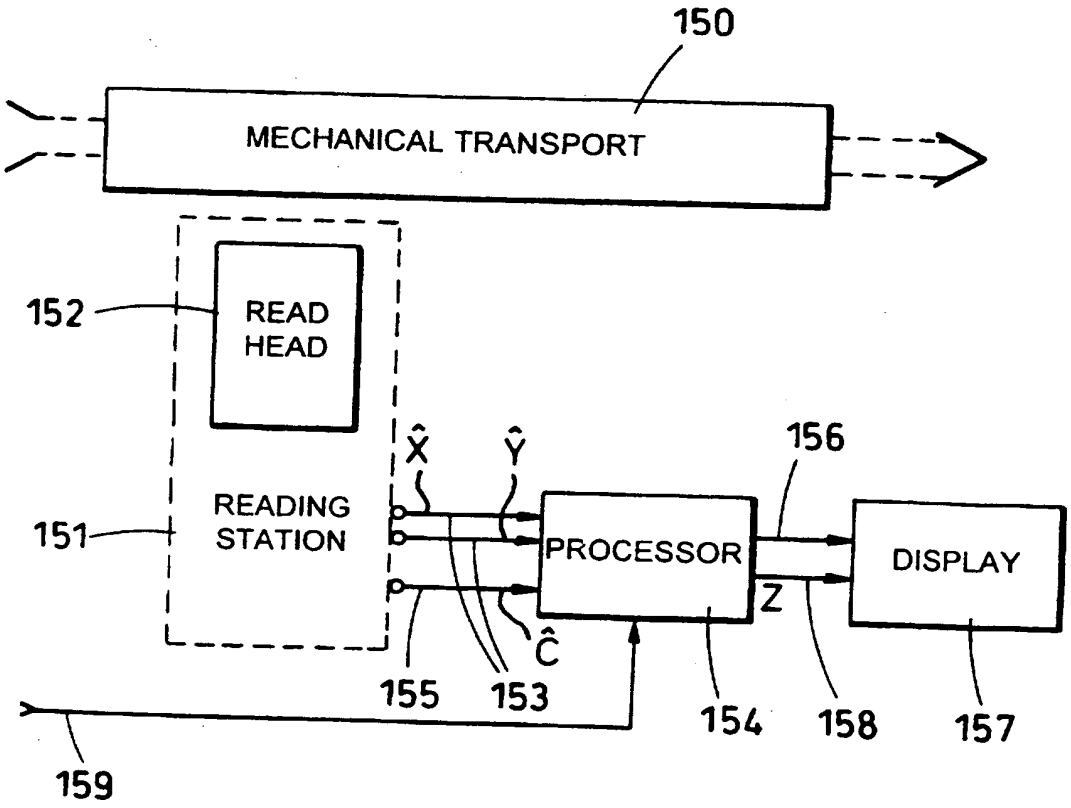

150
MECHANICAL TRANSPORT
152
READ HEAD
151
READING STATION
$\hat{X}$
$\hat{Y}$
$\hat{C}$
156
PROCESSOR
Z
DISPLAY
155
153
154
158
157
159

Fig. 15

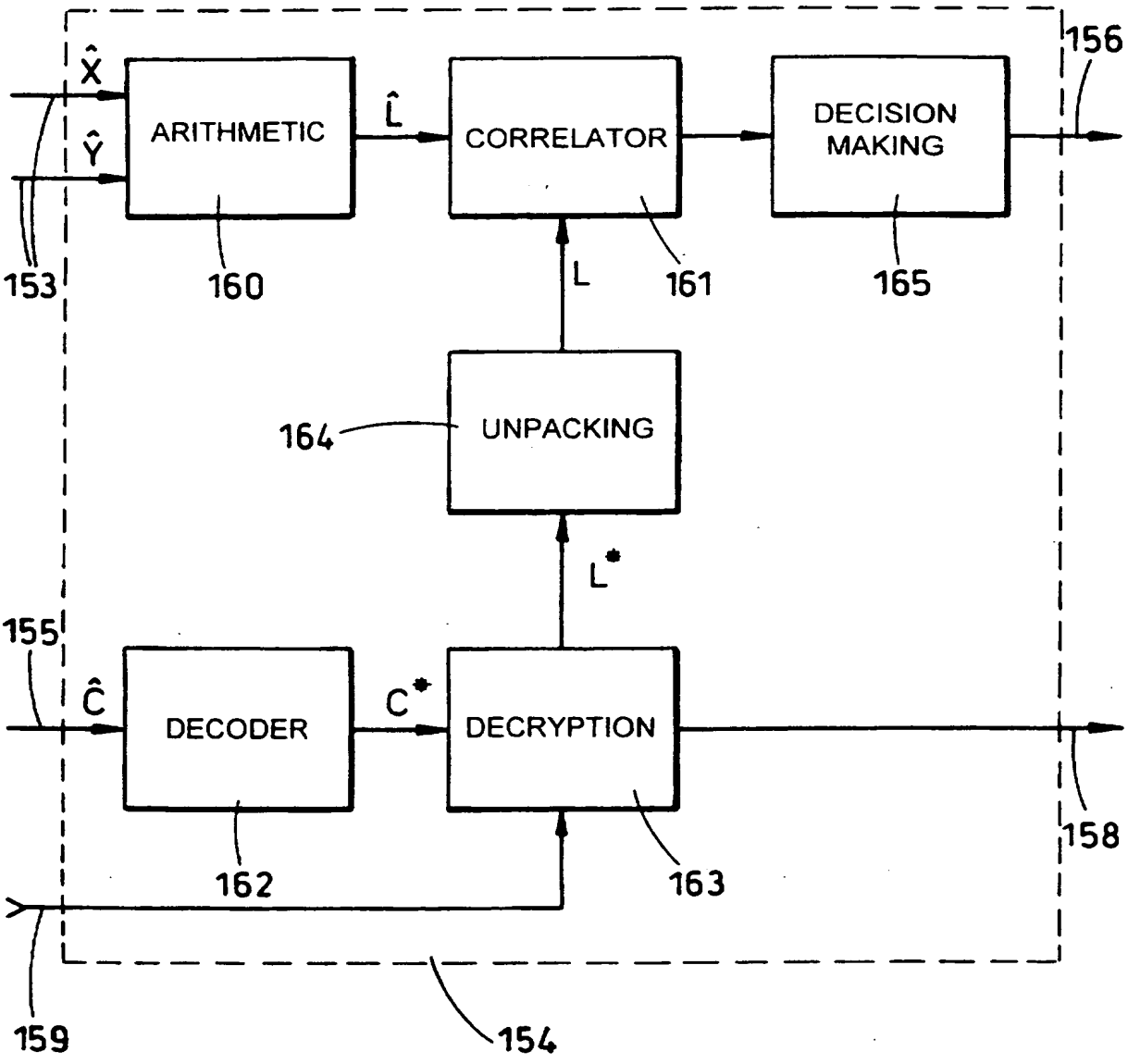

$\hat{X}$
$\hat{Y}$
ARITHMETIC
$\hat{L}$
CORRELATOR
DECISION MAKING
156
153
160
L
161
165
164
UNPACKING
L^*
155
$\hat{C}$
DECODER
C^*
DECRYPTION
158
162
163
159
154

Fig. 16

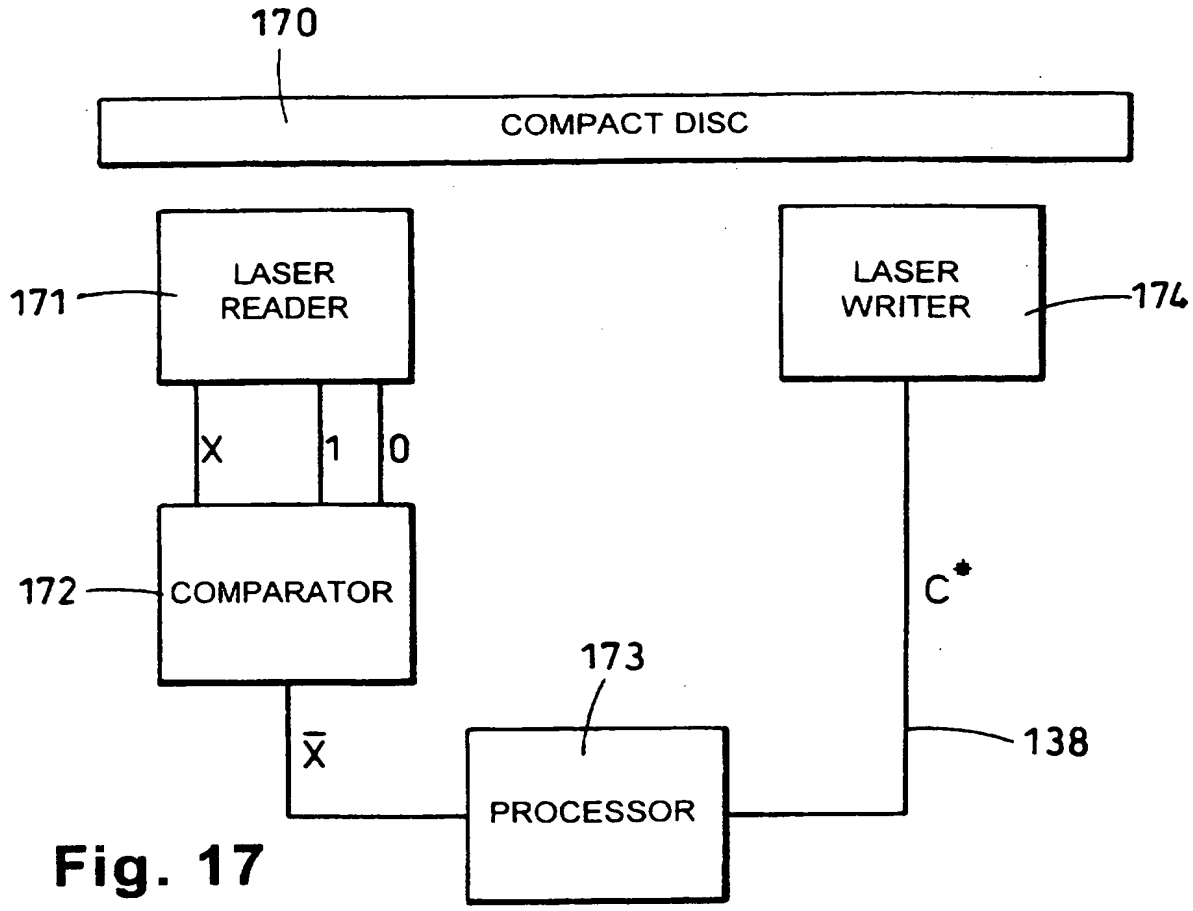

170
COMPACT DISC
LASER READER
171
LASER WRITER
174
X
1
0
172
COMPARATOR
C*
173
$\bar{X}$
PROCESSOR
138

Fig. 17

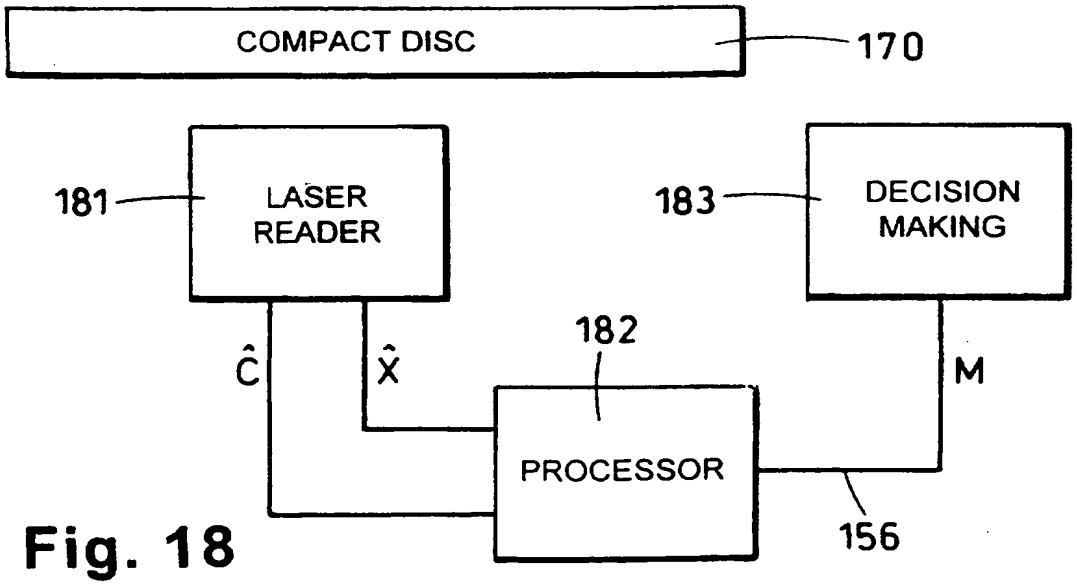

COMPACT DISC
170
181
LASER READER
183
DECISION MAKING
$\hat{C}$
$\hat{X}$
182
M
PROCESSOR
156

Fig. 18

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 95/03051

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07D7/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07D

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US,A,4 218 674 (BROSOW JORGEN ET AL) 19 August 1980	1,16,17, 19,20, 23,30-33
A	see claim 1; figure 1	2-15,18, 21,22, 24-29, 34-49

Y	US,A,4 649 266 (ECKERT ALTON B) 10 March 1987	1,16,17, 19,20, 23,30-33
A	see claim 1; figure 1	2-15,18, 21,22, 24-29, 34-49

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
31 July 1996	13.08.96
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax (+ 31-70) 340-3016	Authorized officer Kirsten, K

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 95/03051

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP,A,0 260 940 (LIGHT SIGNATURES INC) 23 March 1988 see claim 1; figures 1,2	1-49
A	US,A,5 319 705 (HALTER BERNARD J ET AL) 7 June 1994 see claim 1; figure 3	1-49
A	EP,A,0 636 962 (SOFTWARE SECURITY INC) 1 February 1995 see claim 1; figure 1	1-49
A	US,A,4 290 630 (LEE PETER D) 22 September 1981 see claim 1; figure 6	1-49

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB 95/03051

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
US-A-4218674	19-08-80	AU-B-	1726776	09-03-78
		BE-A-	845935	31-12-76
		CH-A-	607168	30-11-78
		DE-A-	2635795	17-03-77
		FR-A-	2324060	08-04-77
		JP-A-	52033444	14-03-77
		NL-A-	7610007	11-03-77
		SE-A-	7609944	10-03-77
US-A-4649266	10-03-87	CA-A,C	1246226	06-12-88
		EP-A-	0154972	18-09-85
		JP-A-	60252994	13-12-85
EP-A-0260940	23-03-88	US-A-	4806740	21-02-89
		CA-A-	1291564	29-10-91
		DE-D-	3751697	21-03-96
		DE-T-	3751697	20-06-96
		JP-A-	63129520	01-06-88
US-A-5319705	07-06-94	JP-A-	7093148	07-04-95
EP-A-0636962	01-02-95	US-A-	5337357	09-08-94
		CA-A-	2120816	18-12-94
US-A-4290630	22-09-81	GB-A-	1580951	10-12-80
		CH-A-	633644	15-12-82
		CH-A-	633900	31-12-82
		DE-A-	2808552	07-09-78
		FR-A,B	2382541	29-09-78
		NL-A-	7802204	05-09-78
		SE-B-	430632	28-11-83
		SE-A-	7802252	02-09-78
		US-A-	4370057	25-01-83